IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. 0.17366943 BITCOIN(BTC), Defendant *in Rem*.	)	CIVIL ACTION NO.: 3:24-988-JFA

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 0.17366943 Bitcoin ("BTC") valued at approximately $8,221 USD ("United States Dollars"), ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(C) made applicable to criminal forfeiture by 28 U.S.C. § 2461(c). The funds described herein are also thereby subject to civil and criminal seizure pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(e) and (f) and 18 U.S.C. § 982(b)(1). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitute, or are traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. §§ 1343 and 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957; and

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consist of 0.17366943 BTC valued at approximately $8,221 USD, obtained by agents with the United States Secret Service ("USSS") during an investigation into a transnational criminal organization running an exploitation of elderly and social engineering scam. The funds were seized from a cryptocurrency custodial wallet under the control of Binance and under the name of Salaman Shahzada.

4. The USSS seized the 0.17366943 Bitcoin BTC Currency valued at approximately $8,221 USD for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $8,221 USD.

KNOWN POTENTIAL CLAIMANTS

6. The known individuals whose interests may be affected by this litigation are:

a. Salaman Shahzada who may have an interest in the Defendant Funds because he was the named account holder from which the Defendant Funds were seized by USSS during this investigation.

BASIS FOR FORFEITURE

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

a. USSS and local law enforcement agencies were investigating a transnational criminal organization running an exploitation of elderly and social engineering scam. In brief summary, investigating agents determined that a scamming group has been using social engineering to contact elderly individuals and convince them that their bank accounts are compromised. Once the scammers have engagement from the victim, they instruct them that their bank accounts are

compromised and that they need to put their funds in a secure location while they investigate. The victims then withdraw their funds in cash and take it to a BTC Automated Teller Machine ("ATM"). From that ATM, the funds are sent to a cryptocurrency wallet address provided by the suspects.

b. Digital currency (also known as virtual currency or cryptocurrency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currencies exhibit properties similar to other currencies, but do not have a physical form, existing entirely on the internet. Digital currency is not issued by any government or bank (in contrast with fiat or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network, often referred to as the blockchain or public ledger. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership or control of illegally obtained proceeds. Bitcoin ("BTC") is one of the most commonly used and well-known digital currencies. Ethereum ("ETH") is another popular and commonly used digital currency.

[1] For purposes of this complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

c. A stablecoin is a digital currency whose market value is attached to or "pegged" to another stable asset. Differing from normal digital currencies, the value of stablecoins are pegged to assets such as fiat currencies like the United States Dollar ("USD") or the Euro, or other types of assets like precious metals or other digital currencies. Stablecoins are thus used to mitigate the volatility in the price of digital currency by mimicking the value of a fiat currency, without actually converting digital currency into fiat. While there are various legitimate uses for stablecoins, they are popular with cyber-criminals who seek to hold digital currency proceeds of crime at a stable or near-fixed value without moving those funds into the legitimate financial system into a fiat currency such as USD. Some examples of stablecoins include:

a. Binance USD (BUSD), which was developed by Binance Holdings Limited and Paxos Trust Company, LLC, is designed to maintain its value at $1.00 USD. BUSD utilizes the existing ETH blockchain.

d. A digital currency exchange (an "exchange") is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. Most exchanges are located outside the boundaries of the United States in order to avoid regulation and

legal requirements, but some popular exchanges operate inside the jurisdiction of the United States. Binance is an example of a popular online exchange that is located outside of the United States but cooperates with and accepts legal process from American law enforcement agencies.

e. A wallet is a means of storing digital currency identified by unique electronic addresses that allows an individual to conduct transactions on the public ledger. To access a wallet on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a digital currency exchanger to make a transaction between digital currency and fiat, or through digital currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

f. What is common across many exploitations of the elderly and elder abuse cases when it comes to cryptocurrency, is that they initially contact the victim from

a point of perceived authority to the victim. They do this through email, text message, and sometimes computer access through a point of compromise such as a virus or clicking a fraudulent link. This can be as sophisticated as impersonating law enforcement or purporting to be from their bank's corporate security. Once the suspect engages with the victims, they often request that they hide or lie about their actions as to not raise suspicion from actual authorities. From this point, they convince the victim to withdraw their own funds from their accounts and forward it to the suspect through various means. A common method it is to have the victim deposit cash into a Bitcoin ATM and send the transaction to a wallet address provided to the victim.

g. Clinton Walker (" Agent Walker") is a Task Force Officer of the United States Secret Service South Carolina Cyber Fraud Task Force (USSS SC CFTF) and have been so employed since January 2023.

h. On December 19, 2023 SLED Investigators were contacted by a compliance specialist of Carolina's Telco Federal Credit Union (CTFCU) in reference to a customer that was the victim of a fraud involving Bitcoin. Agent Walker responded to the CTFCU office located at 110 Outlet Point Blvd, Columbia, S.C. 29210 and met with the reporting party as well as employees of CTFCU. The following description was relayed to Agent Walker as well as a written statement provided by the reporting party. A scheme to defraud the victim occurred between the dates of December 18, 2023 and December 19, 2023 in violation of 18 U.S.C. §§ 1343, 1349

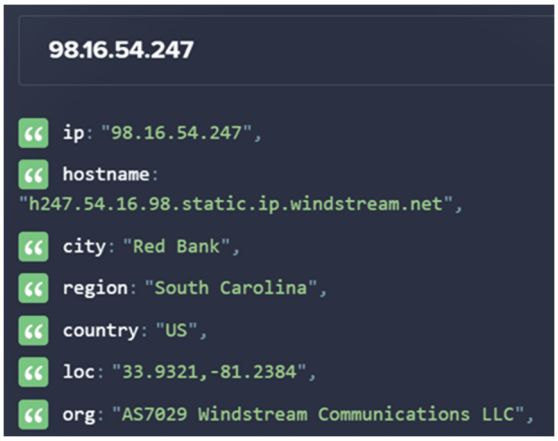
(wire fraud and wire fraud conspiracy) by an unidentified group of subject(s) with the direct involvement and facilitation of Salaman SHAHZADA**.**

i. The reporting victim was transferred between several individuals during the course of the fraudulent scheme. Several subjects provided names and phone numbers while purporting to be affiliated with Etsy.com. All subjects were working in concert to defraud the victim and commit violations of 18 U.S.C. § 1343. The below subjects will be known as Fraud-Ring Members (FM).

Steve Lambert (Account Manager)	1-786-342-1282
Frank (Senior Employee)	1-310-742-4573
Alex Smith (Employee)	1-786-233-1530

j. On December 18, 2023, the Victim attempted to call the customer service line of www.Etsy.com (online retailer of craft goods) to inquire about a refund. The call was placed by the Victim from 133 Cannon Trail Ct, Lexington, S.C. The Victim stated his wife paid $213.00 on the e-commerce site for a custom painting two months prior to placing the call. The items purchased were not received. The Victim attempted to contact Etsy.com customer service and was connected with an individual FM. FM instructed Victim to use his personnel computer to start the refund process. The Victim proceeded to use his personal computer, HP Laptop Model:17-BU4061NR, for the supposed refund activity. The Victim relayed to Agent Walker that he was not very familiar with computers and did not conduct

banking transactions online. Prior to December 18, 2023, the Victim stated that he did not have online banking enabled with CTFCU. Based on information provided from the Victim and representatives of CTFCU, Agent Walker believed that FM(s) connected to the victim's computer through a remote desktop application and created an online banking profile with CTFCU. The remote desktop application enabled FM(s) to make it appear as if the victim was activating the online banking functionality for his accounts. The victim provided FM with the requisite banking information that would allow FM to enroll the victim in online banking through CTFCU. The IP address that was used to create the profile as reported by CTFCU was "**98.16.54.247**". Based on open-source searches, the Internet Protocol address (IP) is registered to Windstream Communications LLC, the victim's internet service provider, and is allocated to an address in the Lexington area consistent with the victim's address.



Opensource information detailing the owner and location assigned to the IP used in the fraud.

k. The victim subsequently submitted the laptop for repair due to the fraudulent activity. A receipt from the repair location indicated 3 instances of unidentified malware located on the machine.

l. With access to the victim's computer and banking account, FM conducted a credit card cash advance of $10,000 from the victim's account. FM told the victim an error was made during the refund process. FM stated $10,000 was refunded to the victim's and money was transferred to the victim's account in error. The victim confirmed, through a call to the automated over the phone balance number, that $10,000 had been transferred into the account. The source of the money was the $10,000 credit card cash advance that FM made against the victim's credit card and transferred to the victim's account. Agent Walker knows this is a common tactic used by fraud subjects. This tactic makes the account appear as though a transfer of outside funds has occurred.

0000210607 S 0015	12/18/2023	12/18/2023	Deposit	Online banking	Transfer	Credit Card Cash Advance: Transfer from L 5101	10,000.00	13,009.09

Victim's banking transactions provided by CTFCU. Transaction on 12/18/2023 depicting a Credit Card Cash Advance 0f $10,000 to the victim's CTFCU checking account.

m. FM instructed the victim to withdraw $9,787 from his checking account and send the money to back to the FM. FM stated the transfer must be completed quickly and indicated to Victim 1 that FM's job was in jeopardy if the funds were

not returned. Based on training and experience, Agent Walker knows this is a common tactic used to illicit finds from victims of fraud.

n. The victim was then directed to the BTMMachines cryptocurrency ATM located at 1601 Broad River Rd, Columbia, S.C. 29210. The ATM is located inside the Halal International market located at the same address. Agent Walker spoke to employees of Halal International market who recalled an individual matching the victim's description using the BTMMachines ATM for approximately 45 minutes.

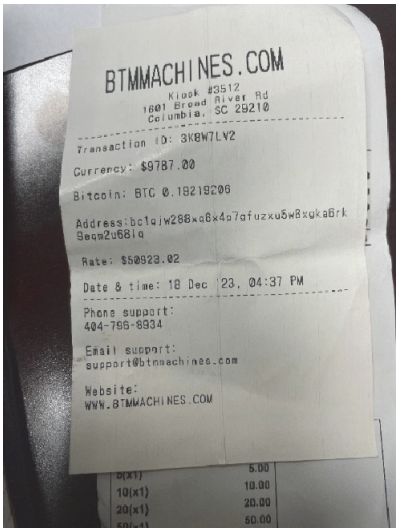
n. The victim was sent a bitcoin address in multiple forms from FM using multiple phone numbers and directed to place the $9,787 withdrawn from the victim's account into the cryptocurrency ATM. The victim received a QR code and subsequent bitcoin address identified as "bc1qjw288xq6x4p7gfuzxu5w8xgka6rk93qm2u68lq'.

o. Victim 1 used the BTMMachines built-in scanner to scan the sent QR code when prompted. Employees of BTMMachines contacted the victim and allowed the transaction to continue. The victim completed the transaction and discontinued communication with FM(s).

p. On December 19, 2023, the victim received a follow up call from FM(s) and was told that an additional transaction had been conducted and the victim would need to send another $11,000. The victim then traveled to the CTFCU branch located at 110 Outlet Point Blvd, Columbia, S.C. 29210. After speaking with an employee of CTFCU, the victim learned he had been the victim of a fraud scheme.

q. Agent Walker was alerted to the fraud and responded to the CTFCU location. He contacted the victim and gathered evidence related to the fraud. FM(s) contacted the victim and requested he travel to the BTMMachines cryptocurrency ATM while in the presence of Agent Walker using multiple numbers. The victim was advised to discontinue contact with FM(s) and employees of CTFCU worked to secure the victim's bank accounts.

r. The victim presented Agent Walker with a BTMMachines.com receipt dated December 18, 2023 at 4:37 PM for the amount of 0.17366943 BTC. Agent Walker spoke with the representatives of BTMMachines.com who confirmed the transaction took place on their machine and stated that they did not have a fee refund policy available to victims of frauds. A BTMMachines representative stated that all AML procedures were followed pursuant to the company's policies and procedures.



Picture of BTMMachines.com transaction receipt provided by the victim.

s. Agent Walker determined that a portion of the funds were transferred to a Cryptocurrency Account using commercially available cryptocurrency tracing software. Agent Walker has received specific training and is certified by the company in the use of the cryptocurrency tracing software.

t. 0.17366943 BTC was deposited into BTC Wallet '*1EJm5ZDX63fjNx6cGKCpqVYoRN2nbVxmA9*' on December 19, 2023. Using commercially available software it was determined that the Cryptocurrency Wallet was associated with Binance. Agent Walker then sent in a legal request for ownership information to Binance requesting the ownership information. Binance returned the ownership and transaction information during the timeframe of the fraud. The owner of the wallet is Salaman SHAHZADA of 107 K Kajiyan, Muzaffarnafar, Uttar Pradesh, India. Transactions dating back to May 27, 2021 in the Cryptocurrency Wallet have been assigned to SHAHZADA. The deposit history provided by Binance matches the information found in the cryptocurrency trace. The Cryptocurrency Wallet at the time of the request was 0.17391943 BTC and a deposit matching the information was found during the cryptocurrency tracing.

BTC	Bitcoin	0.17391943

Target Cryptocurrency Wallet *account balance.*

Currency	Amount	USDT	Deposit Address	Source Address	Create Time
BTC	0.17391304	7594.59637	1EJm5ZDX63fjNx6cGKCpqVYoRN2nbVxmA9	bc1qjw288xq6x4p7gfuzxu5w8xgka6rk9eqm2u68lq	2023-12-20 00:16:32

Target Cryptocurrency Wallet deposit history.

IP address logs provided by Binance were consistent with an individual located in India logging into and out of the Cryptocurrency Account.

u. Agent Walker inspected the information returned from Binance and determined that there was a high likelihood of additional fraudulent activity associated with the Cryptocurrency Account. Agent Walker then conducted law enforcement database searches and discovered two additional reports of fraudulent payments being sent to the Cryptocurrency Account. Both reports were submitted during the period in which SHAHZADA had control over the account.

v. Based on the information gathered during the investigation, Agent Walker obtained a federal seizure warrant for the Cryptocurrency Wallet. This request was honored by Binance and the identified fraudulently obtained funds were transferred into a Binance controlled account and ultimately repatriated to an account controlled by the U.S Secret Service. As such, these funds constitute the Defendant Funs in this complaint.

CONCLUSION

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Currency constitutes, or is traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. §§ 1343 and 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h).

9. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), and 18 U.S.C. § 981(a)(1)(C), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be

issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

Adair F. Boroughs
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

February 27, 2024